

UNITED STATES DISTRICT COURT  
DISTRICT OF MINNESOTA

---

George D., on behalf of himself and as  
legal guardian of his minor child G.D., and  
on behalf of others similarly situated,

Civil No. 19-2814 (JRT/KMM)

Plaintiff,

v.

**MEMORANDUM OPINION AND  
ORDER GRANTING DEFENDANTS'  
MOTION TO DISMISS WITHOUT  
PREJUDICE**

NCS PEARSON, INC. and PEARSON  
EDUCATION, INC., *doing business as*  
*Pearson Clinical Assessment,*

Defendants.

---

Melissa S. Weiner and Joseph C. Bourne, **PEARSON, SIMON & WARSHAW, LLP**, 800 LaSalle Avenue, Suite 2150, Minneapolis, Minnesota 55402; Gary E. Mason and David K. Lietz, **WHITFIELD BRYSON & MASON LLP**, 5101 Wisconsin Avenue NW, Suite 305, Washington, DC 20016; Gary M. Klinger, **KOZONIS & KLINGER, LTD.**, 4849 N. Milwaukee Avenue, Suite 300, Chicago, Illinois 60630, for plaintiffs.

Shannon L. Bjorkland and Stephen P. Lucke, **DORSEY & WHITNEY LLP**, 50 South Sixth Street, Suite 1500, Minneapolis, Minnesota 55402; Jennifer Quinn-Barabanov and Zachary B. Schreiber, **STEPTOE & JOHNSON LLP**, 1330 Connecticut Avenue NW, Washington, DC 20036, Michael Dockterman, **STEPTOE & JOHNSON LLP**, 227 W. Monroe Street, Suite 4700, Chicago, Illinois 60606 for defendants.

In March 2019, Defendants NCS Pearson, Inc. (“NCS Pearson”) and Pearson Education, Inc. (“Pearson Ed”) were notified by the FBI that they had been the victims of a cyberattack compromising one of Defendants’ digital education products. Plaintiff George D. brought claims of negligence, breach of contract, intrusion upon seclusion, and

violation of the Georgia Fair Business Practices Act (“GFBPA”) on behalf of his minor son, G.D., whose personal information is allegedly among the data stolen in the cyberattack, as well as a putative class action for all persons similarly situated. Defendants filed a Motion to Dismiss, arguing that Plaintiff failed to meet the Eighth Circuit’s test for future-harm standing. The Court agrees. Because Plaintiff lacks standing, the Court will grant Defendants’ Motion to Dismiss without prejudice.

## **BACKGROUND**

### **I. FACTUAL BACKGROUND**

Defendants are wholly owned subsidiaries of Pearson PLC, an entity incorporated in the United Kingdom, which Plaintiff describes as “the world’s largest education publisher.” (Am. Compl. ¶ 10, Nov. 25, 2019, Docket No. 12.) Among the technologies offered by Defendants is a platform called AIMSweb. (*Id.* ¶ 12.) AIMSweb is an “educational online progress monitoring and assessment platform.” (*Id.* ¶ 13.)

AIMSweb was licensed by Defendants to “thousands of schools and universit[ies].” (*Id.* ¶ 15.) Plaintiff alleges that G.D. was required by his school district to provide personal information to Defendants via the AIMSweb platform. (*Id.* ¶ 16.) This data included G.D.’s first and last name, his date of birth, email address, and “unique identification number[.]” (*Id.*)

In March 2019, the FBI contacted Defendants and informed them of a cyberattack that had taken place in November 2018. (*Id.* ¶ 19.) This cyberattack allowed an unknown

person or entity to impermissibly access some 13,000 school and university AIMSweb accounts. (*Id.*) As a result, the hacker may have had access to the names, birthdates, and email addresses of individual students. (*Id.* ¶ 21.) Defendants notified institutional account holders of the cyberattack and subsequently offered free credit monitoring to affected individuals. (*Id.* ¶¶ 27, 22.)

## II. PROCEDURAL BACKGROUND

Plaintiff filed his initial complaint on October 30, 2019. (Compl., Docket No. 1.) He brought four counts: (i) negligence; (ii) breach of express contract; (iii) breach of implied contract; (iv) intrusion upon seclusion. (*Id.* ¶ 2.) On November 19, 2019, Plaintiff filed an amended complaint, dropping Pearson PLC as a defendant and adding Pearson Ed as well as a fifth count: violation of the Georgia Fair Business Practices Act. (See Am. Compl. ¶¶ 10, 96–101; Stip., Ex. A at 1, Nov. 19, 2019, Docket No. 5.)

Defendants submitted a Motion to Dismiss on three grounds: (i) Plaintiff lacks Article III standing because he fails to allege an injury-in-fact; (ii) the Court lacks personal jurisdiction over Defendant Pearson Ed; and (iii) Plaintiff has failed to state a claim for each of his five counts. Alternatively, Defendants ask the Court to strike (i) the nationwide class because Plaintiff cannot meet the commonality and predominance requirements of Fed. R. Civ. P. 23; and (ii) the Georgia subclass because the Georgia Fair Business Practices Act prohibits class actions.

## DISCUSSION

### I. STANDING

The Constitution limits federal-court jurisdiction to cases or controversies. *Spokeo, Inc. v. Robins*, 136 S.Ct. 1540, 1547 (2016) (citing U.S. Const. art. II, § 2). Therefore, Plaintiffs must demonstrate standing to sue by showing that they have suffered an injury in fact that is both fairly traceable to the defendant's conduct and likely to be redressed by the relief sought. *Id.*

To establish injury in fact, plaintiffs must show their injury is “‘concrete and particularized’ and ‘actual or imminent, not conjectural or hypothetical.’” *Id.* at 1548 (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992)). During pleading, plaintiffs must allege facts that clearly demonstrate the elements of standing. *Id.* at 1547. When considering a facial attack on a plaintiff's standing under Rule 12(b)(1), the Court accepts the material allegations in the complaint as true and draws all inferences in favor of the plaintiff. *Osborn v. United States*, 918 F.2d 724, 729 n.6 (8<sup>th</sup> Cir. 1990).

The Supreme Court has recognized that future injury can establish Article III standing, but the future injury must be a showing that the future injury is “certainly impending,” or that there is “a substantial risk that the harm will occur.” *Susan B. Anthony List v. Driehaus*, 134 S.Ct. 2334, 2341 (2014) (cleaned up).

## II. ANALYSIS

Plaintiff alleges four imminent or current injuries: (1) the theft of his personal information, (2) the time and costs associated with an increased risk of identity theft, (3) the heightened risk of identity theft, (4) invasion of their privacy, and (5) diminished value of his personal information. (Am. Compl. ¶ 46.)

In regard to the current injuries alleged— theft of personal information, invasion of privacy, and diminished value of personal information—none are sufficiently pleaded.<sup>1</sup> In sum, then, the question before the Court is whether Plaintiff adequately alleges a future injury to confer standing. That is, “whether the complaint adequately alleges that plaintiffs face a ‘certainly impending’ or ‘substantial risk’ of identity theft as a result of the data breach[] purportedly caused by defendants’ deficient security practices.” *In re SuperValu, Inc.*, 870 F.3d 763, 769 (8<sup>th</sup> Cir. 2017).

Even accepting the material allegations as true and drawing all inferences in favor of the Plaintiff, no actual nor imminent injury can be found that is not conjectural or hypothetical. *See Spokeo*, 136 S.Ct. at 1547.

---

<sup>1</sup> The Complaint focuses exclusively on attempting to show future harm, shedding no light on the bases for these additional grounds. As an example of the insufficiency, Plaintiff does not indicate the basis for a claim of invasion of privacy in his Complaint and only in his Opposition does he suggest that the jurisdictional hook is created by the Family Education Rights and Privacy Act (“FERPA”), 20 U.S.C. § 1232g.

To begin, Plaintiff offers no evidence that either the Defendants or the hackers have caused, via his stolen personal information, a current injury-in-fact to G.D. Without evidence of harm caused by use of the stolen information, this Court will not assume that harm has occurred. See *In re SuperValu, Inc.*, 870 F.3d at 769–70 (concluding that plaintiffs’ allegations, on information and belief, that their stolen credit- and debit-card numbers were being sold on the dark web was insufficient to give rise to an injury in fact). Plaintiff instead argues that he has sufficiently alleged future harm because the theft of G.D.’s data creates “increased risk of fraud, identity theft, bullying, shaming, social engineering, tracking, or other means of targeting.” However, the Eighth Circuit rejected a nearly identical claim in *In re SuperValu* and the Court will do the same here. *Id.*

In that case, sixteen named plaintiffs brought a putative class action against a supermarket chain when hackers accessed plaintiffs’ debit- and credit-card information, which had been stored in a payment-processing system maintained by the defendant. *Id.* at 766–67. The Eighth Circuit affirmed dismissal of the case. *Id.* at 774. Regarding the future-harm claims, the panel concluded that because the stolen debit- and credit-card numbers “generally cannot be used alone to open unauthorized new accounts . . . there [was] little to no risk that anyone will use the Card Information stolen in these data breaches to open unauthorized accounts in the plaintiffs’ names.” *Id.* at 770 (internal quotation omitted). The Eighth Circuit also rejected, as the proposed factual basis for the

*SuperValu* plaintiffs’ allegations, the very 2007 report by the Government Accountability Office on which Plaintiff relies in this case.<sup>2</sup> *Id.* at 771.

A difference between *SuperValu* and this case is, however, is that here the stolen data may include one piece of personally identifying information: G.D.’s birthdate. As the Eighth Circuit noted, it was because the “allegedly stolen Card Information does not include any personally identifying information, such as social security numbers, birth dates, or driver’s license numbers” that “there [was] little to no risk that anyone will use the Card Information stolen in these data breaches to open unauthorized accounts in the plaintiffs’ names.” *Id.* at 770. However, as noted above, the evidence on which the Amended Complaint relies for the allegation that G.D.’s birthdate was stolen is ambivalent at best and the Amended Complaint does not resolve this ambiguity by specifically alleging that G.D.’s birthdate was stolen. Even if G.D.’s birthdate was stolen, that piece of information, on its own, does not create a substantial risk that Plaintiff will suffer from identity theft—certainly not a greater risk than a stolen debit- or credit-card number would pose.

---

<sup>2</sup> The Eighth Circuit acknowledged the possibility that “there may be other means—aside from relying on reports and studies—to allege a substantial risk of future injury” and “d[id] not comment on the sufficiency of such potential methods.” *In re SuperValu*, 870 F.3d at 771 n.5. The Plaintiff has not offered any such method here. He points to a blog post, a magazine article, and a public-service announcement produced by the FBI but these three sources all speak to generalized and contingent risks, rather than actual, imminent risk to Plaintiff. (Am. Compl. ¶¶ 25, 30–32, 33–35.)

Likewise, Plaintiff's allegations of an injury derived from the "time and costs associated with dealing with the Data Breach, such as the prevention of future identity theft and the inconvenience, nuisance, and annoyance of dealing with all other issues resulting from the Data Breach" are insufficient. (Am. Compl. ¶ 4, 46.) Because Plaintiff has "not alleged a substantial risk of future identity theft, the time spent protecting . . . against this speculative threat cannot create an injury." *Id.* at 771; *see also Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 416 (2013) (plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending").

Plaintiff fails to meaningfully distinguish his case from *SuperValu*. He devotes much of his briefing to decisions in other circuits that have considered a similar question and come to a different conclusion. But that does not address the question at hand; indeed, the *SuperValu* Court itself noted that other circuits had found standing for similarly situated plaintiffs—but opted to conclude differently. *See id.* at 770 ("[O]thers have ruled that a complaint could plausibly plead that the theft of a plaintiff's personal or financial information creates a substantial risk that they will suffer identity theft sufficient to constitute a threatened injury in fact . . . [but] we conclude that plaintiffs have not done so here.") Although Plaintiff's claim might be sufficiently pleaded to survive a motion to dismiss in other circuits or in state court, he opted to file suit in this circuit.



In sum, the Court is bound by decisions of the Eighth Circuit and Plaintiff has not meaningfully distinguished his case from *SuperValu*, therefore the Court will grant Defendants' 12(b)(1) motion. If, at some future date, evidence of such harm sufficient to confer standing becomes available, Plaintiff could refile his Complaint and possibly meet the *SuperValu* test.

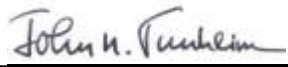
**ORDER**

Based on the foregoing, and all the files, records, and proceedings herein, **IT IS HEREBY ORDERED** that:

1. Defendants' Motion to Dismiss for Lack of Standing [Docket No. 17] is **GRANTED**.
2. Plaintiff's Amended Complaint [Docket No. 12] is **DISMISSED** without prejudice.
3. Intervenor Plaintiff's Motion to Intervene [Docket No. 41] is **DENIED** as moot.

**LET JUDGMENT BE ENTERED ACCORDINGLY.**

DATED: July 6, 2020  
at Minneapolis, Minnesota.

  
\_\_\_\_\_  
JOHN R. TUNHEIM  
Chief Judge  
United States District Court